Industry Spotlight: Legal

The cyber threat landscape has rapidly changed over the last few years for the legal sector, with law firms around the world affected by Maze ransomware and nation-state attacks as threat actors increase their cyber operations. Organizations have been forced to rethink their cyber security strategies and deploy more adaptive defenses that can autonomous respond to emerging attacks.

At a Glance

- ✔ Self-Learning AI understands 'normal' for each user and device
- ✔ Autonomously responds to novel and sophisticated cyber-threats
- ✔ Identifies critical vulnerabilities and misconfigurations
- ✔ Cyber AI Analyst augments and uplifts security teams

THOMMESSEN IceMiller LEGAL COUNSEL Bressler AMERY & ROSS

HOLMAN WEBB LAWYERS CDH CLIFFE DEKKER HOFMEYR Jackson McDonald

SLAUGHTER AND MAY APPLEBY

withersworldwide MURGITROYD

IBB Law taylor | english the purpose-built law firm® Gleiss Lutz

Industry Challenges

Handling large volumes of sensitive data, the legal sector is a perfect target for cyber-criminals. In today's digital world, even the most private legal documents are regularly revised online. From confidential information about M&As to disclosures made under attorney-client privilege, law firms handle data on a daily basis that would be disastrous if leaked, both for the results of individual cases and for these firms' long-term reputations.

Law firms lose on average 5% of their clients following a data breach, while a significant breach can be fatal for a company, as was the case for Mossack Fonseca in 2018 after the leaked Panama Papers. Three years on, ransomware variants like WastedLocker, Maze, and Egregor have raised the stakes higher than ever before.

Double extortion ransomware, where threat actors not only encrypt but also exfiltrate data, adds a further layer of risk to the legal sector, with the possibility that data could be made public on auction sites or online forums on the Dark Web. GDPR fines can cost firms up to 4% of their annual turnover if classified information becomes public knowledge.

Moreover, encrypted data can have a fatal effect on the outcome of legal disputes if essential documents cannot be accessed in time. And paying a ransom is no guarantee of restoring files – around 50% of companies never regain their documents after paying up.

With the pressure of non-compliance and the increasing scale and sophistication of cyber-attacks, now is the time for the legal sector to abandon legacy, signature-based tools in favor of a more advanced approach that uses Self-Learning AI to detect and respond to novel threats.

> "Armed with Cyber AI, we feel strengthened in our fight for data security – we now know we are able to defend against the threats of tomorrow."
>
> Ann Chung, General Manager, ONC Lawyers

Darktrace Self-Learning AI

Darktrace autonomously detects, investigates, and responds to threats in real time. It provides protection and visibility across the entire digital ecosystem, fighting threats on every front – from zero-day exploits on IoT devices, to account compromise on cloud and SaaS platforms, to spear phishing emails in the inbox and beyond.

Law firms across the world rely on Darktrace's Self-Learning AI to protect their critical data and assets. The technology learns the 'pattern of life' for every user and device in an organization, and all the connections between them. Unlike traditional security tools, which rely on some element of an attack to be 'known', Self-Learning AI stops novel attacks on the first encounter by continually updating its understanding of 'normal' and spotting subtle deviations across the digital ecosystem.

Darktrace Antigena then responds to emerging threats with targeted, autonomous action, buying back time for stretched security teams.

Meanwhile, Cyber AI Analyst launches automatic investigations, presenting security teams with all the information they need in concise incident summary reports. The technology augments and uplifts security teams, allowing them to spend more time on proactive and strategic tasks.

Case Study: Stopping Crypto-Jacking and a Botnet Army at K&L Gates

K&L Gates, a global law firm with 45 offices worldwide and gross revenue in excess of $1.2 billion, implemented Darktrace to protect its digital business. The initial installation took under an hour, and Darktrace's AI immediately started developing an understanding of every user and device in the organization.

Soon after installation, Darktrace detected a number of genuine threats, including a covert crypto-jacking operation and the use of a non-compliant VPN that threatened to take corporate devices into the fold of a large botnet army. Darktrace's AI instantly identified these incidents, alerting the security team before this could become a crisis.

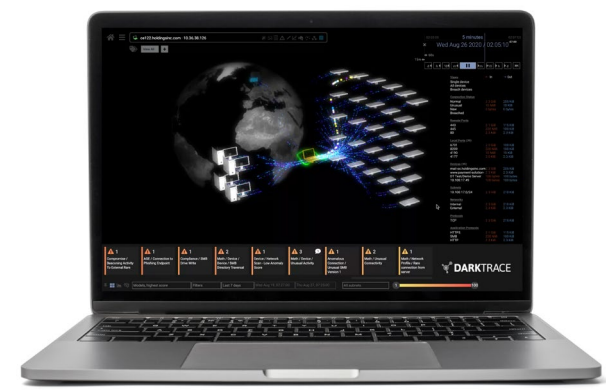
> "Darktrace has enabled us to take our cyber security to a level we presumed unattainable. We can defend our network 24/7 and address unfolding threats before they cause harm."

Asfar Sadewa, Head of IT, Jackson McDonald

Threats by Numbers

of businesses file for bankruptcy within a year of suffering from a major data breach.

of the top 100 law firms have reported that they are regularly attacked by cyber-criminals.



Darktrace Antigena autonomously neutralizes threats, surgically blocking malicious activity